

**IN THE SPECIFICATION**

Please replace the first full paragraph, of page 1 with the following amended paragraph:

This application claims the benefit of U.S. provisional applications 60/138,849, 60/138,850, 60/139,033, 60/139,034, 60/139,035, 60/139,036, 60/139,038, 60/139,042, 60/139,043, 60/139,044, 60/139,047, 60/139,048, 60/139,049, 60/139,052, 60/139,053, all filed on June 10, 1999, and U.S. provisional application 60/139,076, filed on June 11, 1999, the contents of all of which are incorporated herein by reference. This application also contains subject matter that is related to the subject matter disclosed in U.S. Patent Application Nos. 09/591,802, 09/592,079, 09/592,163, 09/592,165, 09/592,442, 09/592,443, 09/591,801 now U.S. Patent no. 6,708,187, and 09/592,083 now U.S. Patent no. 6,678,835.

Please replace the second full paragraph, of page 2 with the following amended paragraph:

As illustrated in FIG. 2, each object in the structure is preferably stored as an LDAP entry. At the top of the hierarchy is the policy server domain object 201 including various policy server resources and a plurality of policy ~~domains~~ domain objects (generally referenced at 204). Each policy domain object 240 is a grouping of policy enforcers that share common policies. Each, policy domain object 240 includes a resource root object 200 and a group root object 202. All policy management functions are preferably implemented in terms of the resource objects, which include devices 204, users 206, hosts 208, services 210, and time 220. Thus, a firewall policy may be defined by simply assigning the particular devices, users, hosts, services, and time applicable to the policy. The devices, users, hosts, and services are preferably organized in groups 212, 214, 216, and 218, respectively, having a group name, description, and member information for a more intuitive way of addressing and organizing the resources.

Please replace the fourth full paragraph, of page 11 with the following amended paragraph:

According to one embodiment of the invention, a policy object 222 includes a bandwidth policy 224, firewall policy 226, administration policy 228 (not shown), and VPN policy 230. The VPN policy 230 defines a security policy for the member networks and includes one or more VPN clouds 232. Each VPN cloud 232 is an individual VPN or a group of VPNs defining a security policy group, which includes a list of sites 234 and users 236 who can communicate with each other. A site is preferably a set of hosts/networks physically located behind one of the policy enforcers 124, 126. In other words, a site is a definition of a network, which includes the policy enforcer that is associated with it. The policy enforcers for the sites act as VPN tunnel endpoints once the hosts under the sites start communicating. These communications are governed by a set of rules 238 configured for each VPN cloud. The rules 238 may govern, among other things, VPN access permissions and security features such as the level of encryption and authentication used for the connectivity at the network layer.

Please replace the first full paragraph, of page 15 with the following amended paragraph:

Once connected, the policy enforcer installation wizard 406 invokes the interactive user interface to assist the network administrator in setting up a particular policy enforcer 124, 126. Among other things, the policy enforcer installation wizard ~~[[464]]~~ 406 prompts the administrator to specify the policy server IP address, policy enforcer IP address, and router IP address. The policy enforcer then registers with the policy server 122 by invoking a URL on the policy server with basic bootstrap information of its own. The registration of the policy enforcer allows the initialization of the policy enforcer's database 132, 134 with the configuration information, as well as the monitoring of the policy enforcer's status and health by the policy server 122.

Please replace the second full paragraph, of page 21 with the following amended paragraph:

Preferably, the user attribute 734 indicates the user groups and users that are eligible for the policy. The source attribute 736 indicates a point of origination of the network traffic

associated with the user. The services attribute 738 indicates the services to [[the]] be allowed or denied by the policy. The destination attribute indicates a specific LAN, WAN, DMS segment or specific hosts where the specified services are to be allowed or denied. For example, to configure SMTP pop services on a mail server, the host may be the IP address where the mail server is running, and the services specified is SMTP. The time attribute indicates a time slot in which the policy is to be effective [[,]] . In addition to the above, each firewall policy also includes an authentication attribute (not shown) indicating an authentication scheme for the policy (e.g. none, LDAP, SecurID, RADIUS, WinNT, or all).

Please replace the first full paragraph, of page 22 with the following amended paragraph:

As illustrated in FIG. 14, a new firewall policy may be defined by simply adding a description of the policy in a description area 728a, selecting an action to be applied to the matching network traffic in an action box 730a, and indicating in an active area 732a whether the policy is to be active or inactive. Furthermore, the network administrator specifies the user, source, services, destination, and time resources in a user area 734a, source area 736a, services area 738a, destination area [[739a]] 739, and time area 741, respectively. The network administrator further selects an authentication scheme for the policy in an authentication area 743. Upon actuation of an OK button 745, appropriate entries of the policy server database's LDAP tree are suitably changed to reflect the addition of the new policy. The change is also transmitted to the respective policy enforcers as is described in further detail below.

Please replace the second full paragraph, of page 33 with the following amended paragraph:

A decision engine 606 includes logic to serve the incoming policy decision requests in the policy request table 602 by matching it against the policy rule set in the policy rules database buffer 608 based on the actual membership information obtained from the resource engine 604. The relevant group-based rule matching the traffic is then identified and decision bits in the stream table are set for enforcing the corresponding actions. The decision bits thus constitute the set of actions to be performed on the packets of the stream. All packets

matching the streams are then processed based on these decision bits. The decision engine may also specify an access control list (ACL) including a set of rules that allow/deny traffic, a DiffServ standard for providing a quality of service level to the traffic, and/or VPN implementation information.

Please replace the second full paragraph, of page 34 with the following amended paragraph:

FIG. 21 is a more detailed schematic block diagram of the IPsec engine 502 according to one embodiment of the invention. As illustrated in FIG. 21, the IPsec engine 502 includes a Pseudo-Random Number Generator (PRNG) function 802 for generating random numbers used for cryptographic key generation according to well known methods. [[A ]] Diffie Hellman 804 and RSA 812 blocks implement the corresponding asymmetric public key encryption/decryption/signature algorithms which are also well known in the art. An IKE block 806 communicates with an IPsec SA table 808 for implementing standard ISAKMP/Oakley(IKE) key a packet was received, as well as a destination IP address and port 826 indicating the destination to which the packet was forwarded.

Please replace the fourth full paragraph, of page 36 with the following amended paragraph:

In addition to the above, each log entry includes an in-bytes field [[832]] 834 indicative of the number of bytes the policy enforcer received as a result of the activity, and an out-bytes field [[834]] 836 indicative of the number of bytes transferred from the policy enforcer. Furthermore, a duration field [[836]] 838 indicates the duration (e.g. in seconds) of the activity.

Please replace the first full paragraph, of page 37 with the following amended paragraph:

A person skilled in the art should recognize that additions, deletions, and other types of modifications may be made to the log format without departing from the spirit and the scope of the invention as long as the log format common to all the policy enforcers [[and]] is

aimed in creating compact logs.

Please replace the second full paragraph, of page 40 with the following amended paragraph:

In step 422, the change made by the administrator is reflected in the policy server database 130. In this regard, branches 264 and 266 of the LDAP tree are modified accordingly to reflect the change in the policy setting. Additionally, in step 424, the policy server 122 creates a log of the changes for the administrator for later processing and sending to the appropriate policy agent. In step 426, the policy server 122 updates the administrator's log DN 270d to reflect the change. In the above example and as illustrated in FIG. 24, if the log created is named "A\_L1," the policy server 122 updates the DN 270d for "adm" at "domain1" to create an attribute "apply" 270f that has the value "A\_L1" 270g. Other changes made by the administrator are reflected in separate logs (e.g. "A\_L2," "A\_L3") and appended to the existing value of the apply attribute in the administrator's log DN 270d.

Please replace the second full paragraph, of page 41 with the following amended paragraph:

The changes suitably modified for each policy enforcer's LDAP are then stored in a device log. Each policy enforcer's log DN 270e is then modified to reflect the change to the transmitted ~~to the~~ particular policy enforcer. In the above example and as illustrated in FIG. 24, if the device log created is named "PE\_L1," the policy server 122 updates the DN 270e for the particular policy enforcer "PE1" at "domain1" to create an attribute "apply" 270i that has the value "PE\_L1" 270j.

Please replace the first full paragraph, of page 44 with the following amended paragraph:

The primary unit 902 responds to the "Keep Alive" packet by changing the command field of the packet to a KEEP\_ALIVE\_RESP command and re-transmitting the packet to the sender. If the backup unit 904 does not receive a response back from the primary unit 902 for

a predetermined period of time (e.g. one second) for one "Keep Alive" packet, the backup unit 904 begins preparing to take over the active role. Preferably, the predetermined period should not be greater less than two consecutive "Keep Alive" packets.

Please replace the first full paragraph, of page 47 with the following amended paragraph:

FIG. 30 is an exemplary flow diagram of updating the primary and backup units when the primary unit is not functional. In step 978, the primary unit becomes nonfunctional, and in step 980, the network administrator sends/transmits an upgrade update directly to the backup unit instead of the primary unit. In step 982, the backup unit updates itself with the information received from the management station and waits for the primary unit to become functional 984. Once the primary unit becomes functional 984 the update is automatically sent/transmitted to the primary unit for upgrading in step 986. The primary unit then updates itself in step 988.

Please replace the Abstract, on page 54 with the following amended paragraph:

#### ABSTRACT OF THE DISCLOSURE

A unified policy management system for an organization including a central policy server and remotely situated policy enforcers. A central database and policy enforcer databases storing policy settings are configured as LDAP databases adhering to a hierarchical object oriented structure. Such structure allows the policy settings to be defined in an intuitive and extensible fashion. Changes in the policy settings made at the central policy server are automatically transferred to the policy enforcers for updating their respective databases. Each policy enforcer collects and transmits health and status information in a predefined log format and transmits it to the policy server for efficient monitoring by the policy server. For further efficiencies, the policy enforcement functionalities of the policy enforcers are effectively partitioned so as to be readily implemented in hardware. The system also provides for dynamically routed VPNs where VPN membership lists are automatically created and shared with the member policy enforcers. Updates to such membership lists are

also automatically transferred to remote VPN clients. The system further provides for fine grain access control of the traffic in the VPN by allowing definition of firewall rules within the VPN. In addition, policy server and policy enforcers may be configured for high availability by maintaining a backup unit in addition to a primary unit. The backup unit ~~become~~ becomes active upon failure of the primary unit.

**Amendments to the Drawings:**

The attached sheets of drawings include corrections to Figs. 2 and 26 as follows: In Fig. 2 reference number 200 referenced in the text, but previously not shown has been added with the appropriate lead line. In Fig. 26, the original reference numbers 502, 504, 506a, 506b, 508, 510, 512, 514, 520a, 520b, 522a, 522b, 524a, and 524b are now corrected to read 902, 904, 906a, 906b, 908, 910, 912, 914, 920a, 920b, 922a, 922b, 924a, and 924b respectively. In addition, 906a and 906b are moved off of the cable 908 and 906a and 906b each have lead lines directed to port element locations with 906a having a lead line directed to the intersection of the primary unit 902 and cable 908 and 906b having a lead line directed to the intersection of the backup unit 904 and cable 908.

Attachment: Replacement Sheet for Figs. 2 and 26  
Annotated Sheets Showing Changes to Figs. 2 and 26 as originally filed.